WHITEPAPER

IT-Outsourcing & Governance

Verantwortung bleibt intern

Warum technische Kontrollen ohne Steuerungsfähigkeit nicht dauerhaft tragen

Carsten Beck

Cybersecurity Auditor | ISO/IEC 27001 & ISO 22301 Lead Auditor

MAS Information Systems Management

Erstveröffentlichung Februar 2026 · Version 1.1 (Oktober 2026)

Executive Briefing

IT-Outsourcing verlagert operative Aufgaben, nicht jedoch die Gesamtverantwortung für Informationssicherheit, Datenschutz und Resilienz der ausgelagerten Leistung. Der Dienstleister trägt eigene Pflichten für die vereinbarte Leistung; die beauftragende Organisation muss ihre Rolle aber auch tatsächlich ausüben können.

Dabei liegen wesentliche Schutzmassnahmen ausserhalb ihrer direkten Kontrolle, und es entstehen Abhängigkeiten von Dienstleistern, Subdienstleistern und Plattformen. Technische Kontrollen bleiben notwendig, tragen aber nur dauerhaft, wenn die Organisation Anforderungen festlegt, die Leistungserbringung überwacht und bei Abweichungen rechtzeitig handeln kann. Diese Steuerungsfähigkeit steht im Mittelpunkt des Whitepapers.

Ein tragfähiger Ansatz umfasst fünf Elemente: klare interne Verantwortung und ausreichende Fähigkeiten, Transparenz über extern bezogene IT-Leistungen und deren Risiken, geeignete vertragliche Instrumente, gelebte Steuerungsprozesse sowie Kontinuitäts- und Exit-Vorsorge. Aus der Kritikalität und dem Schutzbedarf einer Leistung ergeben sich die erforderliche Steuerungsintensität und die Anforderungen an Nachweise. Dazu gehören auch die Beurteilung von Dienstleisterberichten und die Überprüfung der ergänzenden Kontrollen, welche die Organisation selbst umsetzen muss.

Das Whitepaper beurteilt diese Steuerung aus zwei Perspektiven: Design Effectiveness fragt nach ihrer angemessenen Gestaltung, Operating Effectiveness danach, ob sie über einen betrachteten Zeitraum wie vorgesehen angewendet wurde und ob sich das belegen lässt. Dokumentierte Rollen, Verträge und Pläne bilden die Grundlage. Ob sie im Betrieb tragen, zeigt sich an nachvollziehbaren Entscheiden, am Umgang mit Abweichungen und an der überprüften Umsetzung erforderlicher Massnahmen.

Der Beitrag richtet sich an Leitungs- und Aufsichtsgremien sowie an Verantwortliche in Fachbereichen, Governance-, Risiko- und Auditfunktionen. Kapitel 3 beschreibt die fünf Steuerungselemente, Kapitel 4 ihre Prüfung und geeignete Nachweise, Kapitel 5 Leitfragen zur Einschätzung der eigenen Steuerungsfähigkeit.

1 Outsourcing im Kontext systemischer Cyberrisiken

Viele Organisationen verlagern zentrale IT-Services an spezialisierte Dienstleister oder in Cloud-Umgebungen. Damit verändern sich Aufgaben, Zuständigkeiten und technische Architekturen.

Die beauftragende Organisation bleibt jedoch für die ausgelagerte Leistung, für Informationssicherheit, Datenschutz und Resilienz sowie für die Erfüllung ihrer gesetzlichen, aufsichtsrechtlichen und vertraglichen Pflichten verantwortlich. Dies setzt voraus, dass sie den Dienstleister sorgfältig auswählt, klar beauftragt und die Erfüllung der vereinbarten Anforderungen regelmässig überprüft.[1] Der Dienstleister trägt daneben eigene Pflichten für die vereinbarte Leistung. Entscheidend ist, dass die Organisation ihre Verantwortung nicht nur formal behält, sondern tatsächlich wahrnehmen kann.

Lageberichte von Behörden und Fachorganisationen zeigen seit Jahren, dass Dienstleister und Lieferketten bei Cybervorfällen eine erhebliche Rolle spielen. So betraf nach dem Risikomonitor 2025 der FINMA fast die Hälfte der ihr gemeldeten Cybervorfälle im Finanzsektor Drittparteien.[2] Die ENISA beschreibt die wachsenden digitalen Abhängigkeiten als wesentlichen Treiber einer grösseren Angriffsfläche.[3] Besonders relevant sind dabei stark konzentrierte Dienstleisterlandschaften mit potenziellen «Single Points of Failure», komplexe Ketten von Subdienstleistern mit begrenzter Transparenz, Cloud-Abhängigkeiten in kritischen Prozessen sowie die Aggregation sensibler Daten bei wenigen Anbietern.

Diese Faktoren erhöhen die systemische Verwundbarkeit. Outsourcing kann einzelne Risiken durch Spezialisierung und professionelle Leistungserbringung senken. Gleichzeitig entstehen zusätzliche Abhängigkeiten und Risiken entlang externer Wertschöpfungs- und Serviceketten. Bei stark konzentrierten Anbietern können Vorfälle mehrere Organisationen gleichzeitig treffen und systemische Auswirkungen entfalten. Outsourcing reduziert damit die Verantwortung nicht und das Risiko nicht automatisch – es verändert die Art, wie Risiken gesteuert und kontrolliert werden müssen.

Die Risiken bei IT-Outsourcing lassen sich aus drei Perspektiven betrachten, die sich überlagern:

Perspektive	Fokus	Relevanz bei Outsourcing
Informations-sicherheit	Schutzziele: Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit von Informationen und Systemen	Schutz ausgelagerter Daten und Systeme bei eingeschränkter direkter Kontrolle
Cybersicherheit	Bedrohungsakteure, Supply-Chain-Angriffe und Ransomware	Externe Angriffsflächen und systemische Verwundbarkeit entlang der Lieferkette
Datenschutz & Datensicherheit	Datenschutz: Rechte betroffener Personen bei der Bearbeitung von Personendaten; Datensicherheit: TOMs[4] zum Schutz aller Daten	Datenaggregation bei wenigen Dienstleistern; eine Verletzung der Datensicherheit, die Personendaten betrifft, ist zugleich datenschutzrechtlich relevant

Tabelle 1: Perspektiven auf Risiken bei IT-Outsourcing (eigene Darstellung)

[1] Für Personendaten Art. 9 DSG (CH) beziehungsweise, soweit anwendbar, Art. 28 DSGVO. Für Institute in seinem Geltungsbereich hält FINMA-RS 2018/3 «Outsourcing», Rz. 23, fest, dass das Unternehmen gegenüber der FINMA dieselbe Verantwortung trägt, wie wenn es die ausgelagerte Funktion selbst erbringen würde.
[2] FINMA, Risikomonitor 2025, S. 20. Die Angabe bezieht sich auf die der FINMA gemeldeten Cybervorfälle und ist keine allgemeine Quote aller Cybervorfälle.
[3] ENISA, Threat Landscape 2026, 22. September 2026 (Berichtszeitraum Januar bis Dezember 2025).
[4] TOMs = technische und organisatorische Massnahmen; für Personendaten gesetzlich verankert in Art. 8 DSG (CH) und, soweit anwendbar, Art. 32 DSGVO.

ISO/IEC 27001 und NIST CSF 2.0 unterstützen die systematische Steuerung von Informations- und Cyberrisiken. Für ausgelagerte Leistungen sind insbesondere die Controls zu Lieferantenbeziehungen und Cloud-Diensten in ISO/IEC 27001 (Anhang A, 5.19 bis 5.23) sowie die NIST-Kategorie GV.SC zum Management von Cyberrisiken in Lieferketten relevant.

Technische und organisatorische Schutzmassnahmen liegen bei ausgelagerten Leistungen teilweise ausserhalb der direkten Kontrolle der Organisation. Vorfälle können gleichzeitig Verfügbarkeit, Datenintegrität und Rechte betroffener Personen in erheblichem Umfang beeinträchtigen.

Outsourcing ist damit nicht nur eine operative, sondern eine strategische Risikoentscheidung mit potenziell systemischer Wirkung – mit entsprechenden Anforderungen an Governance und Steuerungsfähigkeit.

2 Massnahmen brauchen Steuerung

Technische Schutzmassnahmen wie Verschlüsselung und Backups sowie Prüfungen wie Penetrationstests sind notwendig, adressieren aber nur einen Ausschnitt des Risikobilds. Zertifikate des Dienstleisters nach ISO/IEC 27001, einschliesslich Zertifizierungen auf der Basis von IT-Grundschutz, bescheinigen die Konformität eines Informationssicherheitsmanagementsystems (ISMS) innerhalb eines definierten Geltungsbereichs. Sie ersetzen die eigene Steuerung nicht (vgl. Kapitel 3). In der Praxis wird Cyber- und Informationssicherheit bei Auslagerungen häufig auf solche Einzelmassnahmen und Nachweise reduziert. Das greift zu kurz.

Entscheidend ist nicht allein, ob eine Massnahme existiert, sondern ob die Steuerungsstrukturen vorhanden sind, die sicherstellen, dass sie dauerhaft wirksam bleibt – auch wenn sich Dienstleister, Architekturen oder Bedrohungslagen verändern.

Aus Governance-Perspektive rücken daher andere Fragen in den Vordergrund:

- Wer trägt die Gesamtverantwortung intern – bis hin zu den Leitungs- und Aufsichtsgremien?
- Wie wird die Zusammenarbeit mit Dienstleistern strukturiert gesteuert – über Rollen, Gremien und klare Entscheidwege?
- Wie werden Risiken, Vorfälle und Schwachstellen über Verträge, Reporting sowie Prüf- und Nachweisrechte kontrollierbar gehalten – und sind Eskalationsmechanismen definiert und werden sie genutzt?

Diese Fragen zielen nicht auf einzelne Kontrollen, sondern auf das Design der Steuerungsstrukturen: Rollenmodell, Entscheidprozesse, Regelkreise und Eskalationswege. Erst wenn dieses Design tragfähig ist und gelebt wird, können operative Massnahmen dauerhaft wirken.

Technische Kontrollen ersetzen keine Governance – ihre dauerhafte Wirksamkeit setzt sie voraus.

3 Steuerungsfähigkeit als Kernprinzip

Ob ein Outsourcing-Setup tragfähig ist, zeigt sich an der Steuerungsfähigkeit. Sie bezeichnet die Fähigkeit einer Organisation, Anforderungen an ausgelagerte Leistungen festzulegen, Risiken und Abhängigkeiten zu beurteilen, die Leistungserbringung zu überwachen und bei Abweichungen rechtzeitig wirksame Entscheide zu treffen. Abhängigkeit vom Dienstleister schliesst Steuerungsfähigkeit nicht aus, sie ist gerade der Anlass dafür. Entscheidend ist, ob die Organisation ihre Abhängigkeiten kennt und bewusst steuert oder ihnen ausgeliefert ist.

Steuerungsfähigkeit entsteht im Normalbetrieb und bewährt sich im Vorfall – wenn Entscheide unter Zeitdruck getroffen werden müssen, wenn Informationen fehlen oder wenn Dienstleister unterschiedliche Prioritäten setzen. Dafür braucht die Organisation intern ausreichende Fachkenntnisse, Ressourcen und Entscheidbefugnisse, um Informationen des Dienstleisters beurteilen und notwendige Massnahmen veranlassen zu können. Rollen und Verträge allein schaffen noch keine Steuerungsfähigkeit.

Fünf Elemente sind dabei zentral:

Klares Verantwortungsmodell intern: Die Leitung verantwortet den Steuerungsrahmen. Für jede ausgelagerte Leistung ist ein fachlicher Leistungsverantwortlicher benannt, der Anforderungen, Risiken und Leistungserbringung im Rahmen seiner Befugnisse verantwortet. IT, Informationssicherheit, Datenschutz, Recht und Beschaffung wirken gemäss ihren Mandaten und den festgelegten Entscheid- und Freigabebefugnissen mit; die fachliche Leistungsverantwortung bleibt dabei eindeutig zugeordnet. Die Zuständigkeiten sind abgestimmt – nicht implizit vorausgesetzt. Die interne Revision beurteilt Angemessenheit und Wirksamkeit der Steuerung unabhängig.

Transparenz und risikobasierte Einstufung: Grundlage ist ein vollständiges Inventar der extern bezogenen IT-Leistungen einschliesslich wesentlicher Subdienstleister. Unvollständige Dienstleisterinventare und eine unzureichende Überwachung von Dienstleistern gehören zu den Mängeln, welche die FINMA in ihrer Aufsicht wiederholt festgestellt hat.[5] Die Leistungen werden nach Kritikalität, Schutzbedarf (Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit), Datenarten und potenziellen Auswirkungen bewertet – einschliesslich Datenschutzrisiken für betroffene Personen. Nicht jede Auslagerung erfordert dasselbe Mass an Steuerung; aber jede erfordert eine bewusste Einschätzung. Aus der Einstufung werden die Anforderungen an Auswahlprüfung, Vertragsgestaltung, Reporting, Nachweise, Eskalation sowie Kontinuitäts- und Exit-Vorsorge abgeleitet. Wesentliche Leistungen erfordern eine engere Überwachung und belastbarere Nachweise als Leistungen mit geringer Auswirkung.

Als wesentlich gelten in diesem Whitepaper Leistungen, deren Ausfall, Kompromittierung oder Schlechterfüllung erhebliche Auswirkungen auf die Leistungserbringung, den Schutz der Informationen, betroffene Personen oder die Erfüllung gesetzlicher und vertraglicher Pflichten hätte. Sektorspezifische Definitionen, etwa der FINMA, gehen dieser Arbeitsdefinition vor. Zur Einstufung gehört auch der Blick auf Konzentrationen: auf Dienstleister, bei denen sich wesentliche Leistungen bündeln, und auf gemeinsame technische Abhängigkeiten verschiedener Dienstleister.

Vertragliche Steuerungsinstrumente: Sicherheitsanforderungen, Prüf- und Nachweisrechte, Reportingpflichten sowie Regelungen zu Vorfällen und Exit-Szenarien sind vertraglich verankert. Hinzu kommen Mechanismen zur Anpassung bei veränderter Bedrohungslage oder geänderten Geschäftsanforderungen. Für Subdienstleister sind Transparenz, die Information über Änderungen, die Weitergabe relevanter Anforderungen und geeignete Nachweismöglichkeiten geregelt. Bei einer Auftragsbearbeitung bedarf die Unterbeauftragung zudem der vorgängigen Genehmigung der beauftragenden Organisation.

Gelebte Gremien und Prozesse: Regelmässige Steuerungsgespräche, nachvollziehbare Entscheide, die Bearbeitung von Risiken und Prüfungsergebnissen sowie klare Eskalationswege sichern die laufende Steuerung. Zertifikate und unabhängige Prüfberichte, etwa SOC-2-Berichte oder nach ISAE 3000 (Revised) auf Grundlage geeigneter Sicherheitskriterien erstellte Berichte, sind auf ihre Aussagekraft für die bezogene Leistung zu prüfen. Relevant sind Geltungsbereich, Prüfkriterien, Prüfungssicherheit, Prüfzeitpunkt oder Prüfzeitraum, abgedeckte Kontrollen, Feststellungen und die Behandlung von Subdienstleistern. Zusätzlich sind die ergänzenden Kontrollen zu bestimmen, welche die beauftragende Organisation selbst umsetzen muss.

[5] FINMA-Aufsichtsmitteilung 03/2024, Abschnitt 2.1.

Kontinuitäts- und Exit-Vorsorge: Kontinuitätsvorsorge sichert die Leistung bei einer Unterbrechung, Exit-Vorsorge ermöglicht eine geordnete Beendigung, Übertragung oder Rückführung. Für wesentliche Leistungen werden Ausweich- oder Notbetrieb und Wiederanlauf mit den Anforderungen der betroffenen Prozesse abgestimmt. Daneben werden die geordnete Übertragung oder Rückführung, die Verfügbarkeit der benötigten Daten und die dafür erforderlichen Ressourcen vorbereitet. Die Umsetzbarkeit wird risikogerecht durch Übungen oder geeignete Teiltests überprüft.

Steuerungsfähigkeit zeigt sich daran, ob kritische Entscheide – bei Sicherheitsvorfällen, Verletzungen der Datensicherheit, Schwachstellen oder Kapazitätsproblemen – zeitnah, nachvollziehbar und auf Basis belastbarer Informationen getroffen werden können. Fehlt diese Handlungsfähigkeit, ist zu untersuchen, ob die Ursache im Steuerungsdesign, in dessen Umsetzung, in der Leistung des Dienstleisters oder im Zusammenspiel dieser Faktoren liegt.

4 Wirksamkeit der Steuerung

Die Wirksamkeit der in Kapitel 3 beschriebenen Steuerung wird aus zwei Perspektiven beurteilt: Design Effectiveness untersucht ihre angemessene Gestaltung, Operating Effectiveness ihre Anwendung wie vorgesehen über einen betrachteten Zeitraum, belegt durch belastbare Nachweise. Tabelle 2 stellt beide Perspektiven anhand der fünf Steuerungselemente gegenüber.

Design Effectiveness	Operating Effectiveness
Verantwortungsmodell: Leitung, fachliche Leistungsverantwortliche, Befugnisse und Stellvertretungen sind festgelegt; die Mitwirkung der Kontrollfunktionen ist geregelt.	Leistungsverantwortliche treffen Entscheide und bearbeiten Eskalationen; die Entscheide sind nachvollziehbar dokumentiert.
Transparenz und risikobasierte Einstufung: Ein Inventar der extern bezogenen IT-Leistungen einschliesslich wesentlicher Subdienstleister, die Einstufungskriterien und die daraus folgenden Steuerungsanforderungen sind festgelegt.	Inventar und Einstufungen werden aktualisiert; neue Dienstleister, Änderungen und neue Abhängigkeiten werden bewertet. Erforderliche Anpassungen der Steuerung werden nachweisbar umgesetzt.
Vertragliche Steuerungsinstrumente: Sicherheitsanforderungen, Reporting, Prüf- und Nachweisrechte, Meldepflichten sowie Regelungen zu Subdienstleistern und Exit sind vertraglich verankert.	Prüf- und Nachweisrechte werden risikogerecht genutzt; Abweichungen von vertraglichen Anforderungen werden erkannt und mit den vereinbarten Instrumenten behandelt.
Gelebte Gremien und Prozesse: Gremien, Entscheidwege und Eskalationsstufen sind definiert; die Auswertung von Reports und Dienstleisternachweisen sowie die Nachverfolgung von Feststellungen sind geregelt.	Gremien behandeln relevante Abweichungen und veranlassen Massnahmen; diese werden innerhalb vereinbarter Fristen umgesetzt und auf ihre Wirksamkeit überprüft. Eskalationen erreichen die zuständige Ebene.
Kontinuitäts- und Exit-Vorsorge: Für wesentliche Leistungen sind Kontinuitäts- und Exit-Szenarien, Zuständigkeiten, benötigte Daten und Ressourcen vorbereitet.	Übungen oder geeignete Teiltests belegen die Umsetzbarkeit; erkannte Lücken werden bearbeitet; die Pläne werden bei Änderungen aktualisiert.

Tabelle 2: Design Effectiveness und Operating Effectiveness der Outsourcing-Steuerung (eigene Darstellung)

Beide Perspektiven ergänzen sich: Eine angemessene Gestaltung schafft die Grundlage für wirksame Steuerung. Ob diese im Betrieb trägt, muss über einen betrachteten Zeitraum durch belastbare Nachweise belegt werden. In frühen Phasen einer Auslagerung steht die Gestaltung im Vordergrund; im laufenden Betrieb sind Gestaltung und Anwendung gemeinsam zu beurteilen.

Prüfnachweise: Nachweise müssen erkennen lassen, ob die in Tabelle 2 beschriebenen Anforderungen über den betrachteten Zeitraum erfüllt wurden. Dass ein Gremium tagt oder eine Massnahme beschlossen wird, belegt zunächst Aktivität. Wirksamkeit zeigt sich daran, dass relevante Abweichungen angemessen behandelt, erforderliche Massnahmen umgesetzt und deren Ergebnisse überprüft werden.

5 Leitfragen für Leitungs- und Aufsichtsgremien

Für Leitungs- und Aufsichtsgremien steht weniger die Frage nach einzelnen technischen Details als vielmehr der Zustand der Governance insgesamt im Vordergrund: Ist die Organisation in der Lage, Risiken und Leistungen ihrer Dienstleister tatsächlich zu steuern – und kann sie das im Bedarfsfall belegen?

Die folgenden Leitfragen dienen der Einschätzung:

- Ist transparent dokumentiert, welche IT-Leistungen von Dienstleistern und Cloud-Anbietern erbracht werden, welche davon wesentlich sind und welche Datenarten und Subdienstleister betroffen sind?
- Liegt eine nachvollziehbare Risikoeinschätzung dieser Leistungen vor, inkl. Konzentrationsrisiken, Cloud-Abhängigkeiten und datenschutzrechtlicher Risiken?
- Verfügt die Organisation über geeignete Steuerungsinstrumente: Verträge, Reporting, Prüf- und Nachweisrechte und Exit-Planung?
- Besteht ein konsistentes Rollen- und Gremienmodell für die Steuerung von Auslagerungen mit benannten Leistungsverantwortlichen und ausreichenden internen Fähigkeiten – und wird es aktiv genutzt?
- Werden kritische Vorfälle und Schwachstellen in ausgelagerten Umgebungen systematisch ausgewertet, und führen sie zu nachweisbaren Anpassungen?
- Ist der definierte Risikoappetit mit den getroffenen Auslagerungsentscheidungen vereinbar – insbesondere im Hinblick auf Datenaggregation und mögliche Auswirkungen auf betroffene Personen?
- Ist sichergestellt, dass die Organisation bei Ausfall oder Wegfall eines wesentlichen Dienstleisters handlungsfähig bleibt – und werden die Kontinuitäts- und Exit-Vorkehrungen durch Übungen oder Teiltests überprüft?
- Welche Nachweise könnten wir heute dafür vorlegen, dass unsere Steuerung nicht nur dokumentiert ist, sondern im Betrieb wirkt?

Die Antworten liefern einen Ausgangspunkt für das nächste Governance-Review und gezielte Verbesserungen im eigenen Steuerungsmodell.

Fazit

IT-Outsourcing ist für viele Organisationen zentral für die Leistungserbringung – und zugleich eine strategische Risikoentscheidung. Technische Sicherheitsmassnahmen sind notwendig, aber nicht hinreichend. Entscheidend ist, dass die Verantwortung für Informationssicherheit, Datenschutz und Resilienz nicht nur formal bei der Organisation verbleibt, sondern tatsächlich wahrgenommen wird.

Ein tragfähiger Ansatz verbindet deshalb fünf Elemente:

- klare interne Verantwortung mit den dafür nötigen Fähigkeiten,
- transparente und risikogerecht eingestufte Leistungen,
- geeignete vertragliche Instrumente,
- eine im Betrieb nachweisbar wirksame Steuerung sowie
- eine Kontinuitäts- und Exit-Vorsorge, die die Handlungsfähigkeit bei Unterbrechung oder Wegfall eines Dienstleisters sichert.

Steuerungsfähigkeit ist kein Selbstzweck. Sie ist die Voraussetzung dafür, dass eine Organisation im Vorfall handlungsfähig bleibt, Entscheide auf belastbarer Grundlage trifft und ihrer Verantwortung gegenüber Kundinnen und Kunden, Mitarbeitenden und weiteren Betroffenen gerecht wird.

Outsourcing verschiebt Aufgaben. Die Gesamtverantwortung bleibt intern.

Quellen

AICPA: 2017 Trust Services Criteria (With Revised Points of Focus – 2022).

DSG, SR 235.1: Datenschutzgesetz vom 25. September 2020, Art. 8 und 9.

DSGVO, Verordnung (EU) 2016/679: Datenschutz-Grundverordnung vom 27. April 2016, Art. 28 und 32.

ENISA: Threat Landscape 2026, 22. September 2026.

FINMA, Aufsichtsmitteilung 03/2024: Erkenntnisse aus der Cyber-Risiko-Aufsichtstätigkeit, 7. Juni 2024, Abschnitt 2.1.

FINMA: Risikomonitor 2025, S. 20.

FINMA, Rundschreiben 2018/3: Outsourcing, Rz. 23.

IAASB, ISAE 3000 (Revised): Assurance Engagements Other than Audits or Reviews of Historical Financial Information, 2013.

ISO/IEC 27001:2022: Information security management systems. Requirements, Anhang A, Controls 5.19 bis 5.23.

NIST: The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, Februar 2024, Kategorie GV.SC.

Hinweis

Dieses Whitepaper gibt ausschliesslich meine persönliche fachliche Einschätzung wieder und steht nicht für eine Behörde oder Aufsicht. Es darf unverändert weitergegeben und mit Quellenangabe zitiert werden. Kommerzielle Verwertung und Bearbeitungen bedürfen meiner vorherigen Zustimmung.



Fragen und Austausch willkommen

carsten@carsten-beck.ch

Alle Beiträge der Reihe

carsten-beck.ch/publikationen

linkedin.com/in/carstenbeck-grc